ETSI
The Standards People

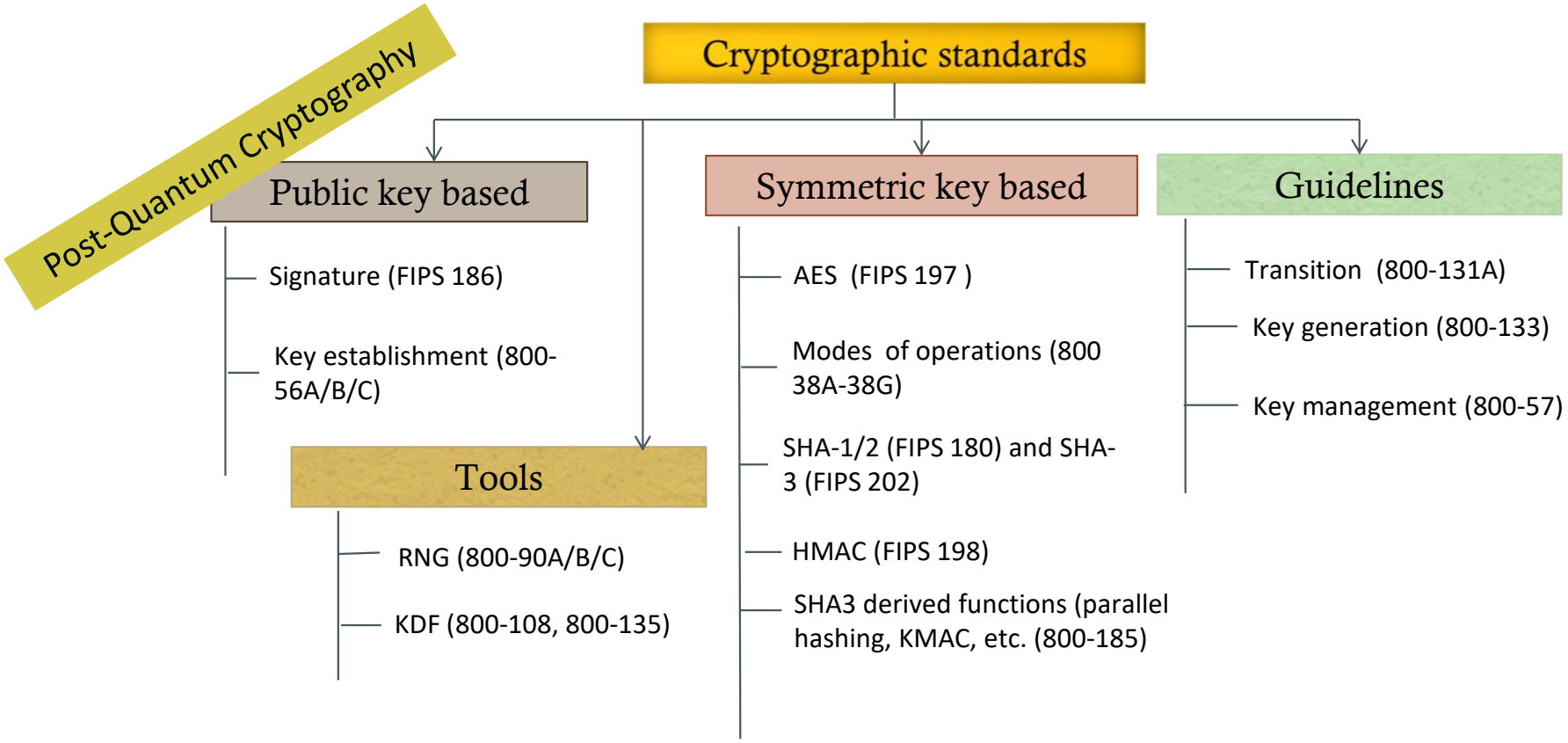
Security Conference

Update on the NIST PQC Standards

Presented by: Lily Chen

10/17/2023

NIST Cryptographic Standards and PQC Scope



NIST PQC Standards – Milestones and Timeline

2016 Criteria and requirements and call for proposals

2017 Received 82 submissions and announced 69 1st round candidates

2018 The 1st NIST PQC standardization Conference

2019 Announced 26 2nd round candidates

The 2nd NIST PQC Standardization Conference

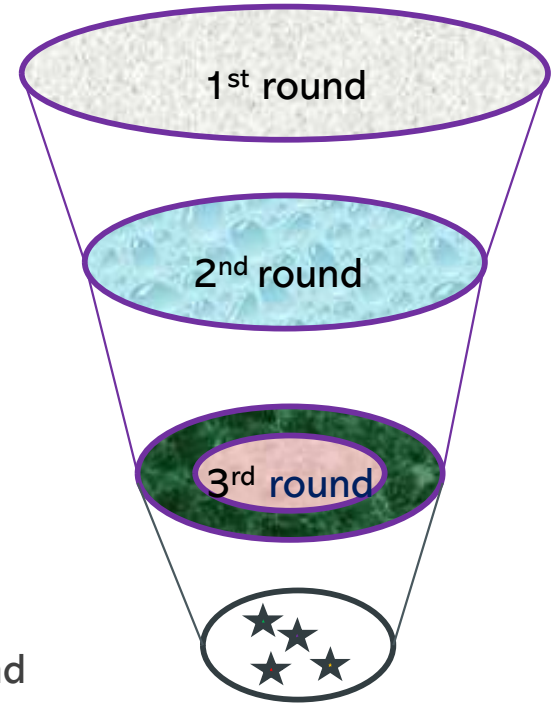
2020 Announced 3rd round 7 finalists and 8 alternate candidate

2021 The 3rd NIST PQC Standardization Conference

2022 Announced the 3rd round selection and the 4th round candidates

2023 Release draft standards for public comments

2024 Publish the 1st set of PQC Standards



Current Status

	Digital Signature	Key Encapsulation (KEM)
Approved	SP 800-208 Stateful Hash-Based Signature (LMS, XMSS)	
Selected Algorithms	• CRYSTALS-Dilithium: Draft FIPS 204 (released) • SPHINCS+: Draft FIPS 205 (released) • Falcon: Draft FIPS 206 (under development)	• CRYSTALS-Kyber: Draft FIPS 203 (released)
The 4th Round Candidates		• Classic McEliece • BIKE • HQC • ~~SIKE~~
Onramp signatures	• 40 candidates are under analysis and evaluation	

NIST SP 800-208: Recommendation for Stateful Hash-Based Signature Schemes

- Stateful hash-based signatures were proposed in 1970s
  - Rely on security of hash functions, not on number theory complexity assumptions
  - It is essentially one-time signature and requires careful state management
- Stateful hash-based signatures were not included in NIST PQC call for submissions, while they are specified in IETF RFCs
  - [1] RFC 8391 XMSS: eXtended Merkle Signature Scheme (2018)
  - [2] RFC 8554 Leighton-Micali Hash-Based Signatures (2019)
- NIST SP 800-208 approves the use of some but not all of the parameter sets defined in [1] and [2] and also defines some new parameter sets
- Stateful hash-based signature is for implementations which have a long-life cycle and need to be quantum ready now
  - The stateful hash-based signatures are used for signing software/firmware

- "Stateful HBS schemes are not suitable for general use because they require careful state management …" — SP 800-208

The Selected Algorithms and Draft Standards

- CRYSTALS-KYBER
  - Key Encapsulation Mechanism (KEM) based on structured lattices
  - Specified in Draft FIPS 203 “Module-Lattice-based Key-Encapsulation Mechanism Standard” (ML-KEM)
- CRYSTALS-DILITHIUM
  - Digital signature based on structured lattices
  - Specified in Draft FIPS 204 “Module-Lattice-Based Digital Signature Standard” (ML-DSA)
- SPHINCS+
  - Stateless hash-based signature
  - Specified in Draft FIPS 205 “Stateless Hash-Based Digital Signature Standard” (SLH-DSA)
- FALCON
  - Digital signature based on structured lattices
  - Will be specified in Draft FIPS 206

- Draft FIPS 203, 204, and 205 were released for public comments on August 17, 2023
  - The comment period ends November 22, 2023
- Draft FIPS 206 is under development and expected to be released in 2024 for public comments

The 4th Round Candidates

- Classic McEliece
  - NIST is confident in the security
  - Smallest ciphertexts, but largest public keys
  - We'd like feedback on specific use cases for Classic McEliece
- BIKE
  - Most competitive performance of 4th round candidates
  - We encourage vetting of IND-CCA security
- HQC
  - Offers strong security assurances and mature decryption failure rate analysis
  - Larger public keys and ciphertext sizes than BIKE
- SIKE
  - The SIKE team acknowledges that SIKE (and SIDH) are insecure and should not be used

Onramp Signatures

- Why NIST called for additional post-quantum signatures?
  - NIST is primarily interested in additional general-purpose signature schemes that are not based on structured lattices.
  - NIST may also be interested in signature schemes that have short signatures and fast verification.
  - Any lattice signature would need to significantly outperform CRYSTALS-Dilithium and FALCON and/or ensure substantial additional security properties.
- Received 50 submissions – 40 of them are accepted as the first-round candidates

Multivariate		MPC in-the-head				Lattice	Code	Symmetric	Isogeny	Other
UOV	Other	MinRank	SD/Rank-SD	PKP	MQ					
Mayo	3wise	Mira	RYDE	Perk	MQOM	EagleSign	Enh. Pqsig-rm	Aimer	SQIsign	Alteq
PROV	DMEsign	MiRitH	SDitH		Biscuit	EHT	Fuleeca	Ascon-sign		eMLE-Sig 2.0
QR-UOV	HPPC					HAETAE	LESS	FAEST		KAZ
SNOVA						Hawk	MEDS	SPHINCS-alpha		Preon
TUOV						HuFu	Wave			Xifrat
UOV						Raccoon	Cross			
Vox						Squirrels				
7	3	2	2	1	2	7	6	4	1	5
10		7								
40										

Besides FIPS Publications,

- Besides FIPS publications for PQC, NIST plans to provide additional guidelines and requirements in special publications
  - For FIPS 203 Module-Lattice-based Key-Encapsulation Mechanism Standard, NIST team is developing Special Publication 800-227 "Recommendations for key-encapsulation mechanisms" to specify security requirements when used in key establishment protocols
  - For FIPS 205 "Stateless Hash-Based Digital Signature Standard", NIST may consider to approve a version of SPHINCS+ through an SP, which allows a smaller maximum number of signatures (Current draft FIPS 205 requires to allow a maximum of 2^{64} signatures)
  - For FIPS 204 and FIPS 206, if additional guidelines and requirements are needed, SPs will be considered as additional publications

- NIST will host the 5th NIST PQC Standardization Conference
  - April 10-12, 2024, in Rockville, Maryland
  - The purpose of the conference is to discuss various aspects of the algorithms (both those selected and those being evaluated)
  - Submission deadline: January 26, 2024

Migration to PQC - NCCoE Project

Consortium Members

These companies are working together to develop actionable guidance for PQC migration:

Amazon Web Services, Inc. (AWS)
Cisco Systems, Inc.
Crypto4A Technologies, Inc.
CryptoNext Security
Dell Technologies
DigiCert
Entrust Corporation
IBM
Infosec Global
ISARA Corporation
JPMorgan Chase Bank, N.A.
Microsoft
Samsung SDS Co., Ltd.
SandboxAQ
Thales DIS CPL USA, Inc.
Thales Trusted Cyber Technologies
Vmware, Inc.
wolfSSL

Working to ease the migration from the current set of public-key cryptographic algorithms to quantum-resistant algorithms.

DISCOVERY WORKSTREAM

Bringing together discovery tools to detect and report the presence and use of quantum vulnerable cryptography with enough detail and context to inform risk analysis and remediation.

INTEROPERABILITY WORKSTREAM

Identifying the challenging problems and bottlenecks that one will face when implementing the first algorithms NIST will standardize as a result of the PQC Standardization Process.

PERFORMANCE WORKSTREAM

Measuring the performance of classical, PQC, and PQ-hybrid use cases across multiple protocols and test conditions.

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

PROJECT GOALS

- Align and complement the NIST PQC standardization activities.
- Develop practices to ease the migration from the current set of public-key cryptographic algorithms to replacement algorithms that are resistant to cryptanalytically relevant quantum computer (CRQC) attacks.
- Deliver white papers, playbooks, and demonstrable implementations for organizations that provide cryptographic standards and protocols and enterprises that develop, acquire, implement, and service cryptographic products.

Coordinate with International Standards

- ISO/IEC JTC1 SC27
  - Stateful hash-based signatures are specified in ISO/IEC 14888-4
    - It is in the stage of DIS (draft information standard)
  - The 1st WD of ISO/IEC 18033-2 “Information technology — Security techniques — Encryption algorithms — Part 2: Asymmetric ciphers” Amendment 2 includes
    - Classic McEliece (a NIST 4th round candidate)
    - FrodoKEM (an alternative candidate in NIST 3rd round)
    - CRYSTALS-Kyber (NIST selected and specified in draft FIPS 203)

Check out www.nist.gov/pqcrypto

Sign up for the pqc-forum for announcements & discussion

send e-mail to pqc-comments@nist.gov